Annals of Nuclear Energy 112 (2018) 646–654

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept

Chanyoung Lee [a], Ho Bin Yim [b], Poong Hyun Seong [a,*]

[a] Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291, Gwahak-ro, Yuseong-gu, Daejeon 305-701, Republic of Korea
[b] Department of Safety Analysis, KEPCO E&C Co., Inc., 989, Daedeok-daero, Yuseong-gu, Daejeon 34057, Republic of Korea

ARTICLE INFO

Article history:
Received 1 June 2017
Received in revised form 31 October 2017
Accepted 2 November 2017

Keywords:
Security control
Intrusion tolerant strategy
Intrusion tolerance based measure
Cyber security index
Mean Time To Compromise

ABSTRACT

Many regulatory documents, guides, and standards for cyber security issues in the nuclear industry have been published since Digital Instrumentation and Control (DI&C) systems were introduced to Nuclear Power Plants (NPPs). However, there are still difficulties when it comes to deciding which security controls are needed and to defining appropriate security control requirements for NPPs. With these regard, a quantitative method for evaluating the efficacy of security controls for DI&C systems in NPPs based on the intrusion tolerant concept is proposed in this study. The essence of the suggested method, ***In***trusion ***To***lerance based ***C***yber ***S***ecurity ***I***ndex (*InTo-CSI*), is defined as a reduction ratio of probability that a cyber-attack damages a target system. The intrusion tolerant concept is applied to the evaluation method because availability of system's safety functions is the first priority in the nuclear industry. "How much the system is intrusion-tolerant" means that to what extent does the system provide the minimum level of safe operation when facing unexpected intrusions. Based on intrusion tolerant strategies, an event tree was constructed, and *InTo-CSI* was estimated by failure probability of intrusion tolerant strategies: the resistance strategy, the detection strategy, and the graceful-degradation strategy. Among these three strategies, quantifying failure probability of the resistance strategy is more challenging than the other two strategies because its relation with attack-difficulty. Attack-difficulty has a strong dependence on unexpected and abstract factors such as attacker's skills and accessibility to information of the target system. For this reason, the model of Mean Time To Compromise (MTTC) was adopted to estimate abstract variables, and the adopted model was revised in accordance with the suggested evaluation method. Validity of the suggested method was proven by conducting a case study. The suggested method can help assess how much the system security can be improved by applying specific cyber security controls, and which types of additional cyber security controls should be taken. Furthermore, *InTo-CSI* can make security designers achieve efficacy levels of the specific target system by quantitatively evaluating cyber security controls.

1. Introduction

Digital Instrumentation and Control (DI&C) systems have been developed and installed in Nuclear Power Plants (NPPs). This introduction of DI&C has brought up a new issue of cyber security, and concerns are continuously growing in the nuclear industry. Actually, DI&C systems of NPPs are physically isolated from external networks, thus NPPs are regarded as the safe stand-alone system from external cyber-attacks. Consequently, cyber security has received less attention than other safety problems have (Kim, 2014). However, continuous attempts of cyber-attacks against NPPs signified that NPPs are as susceptible to the cyber-attack as other safety critical infrastructures, so the public perception of cyber security for NPPs has been changing (Park and Suh, 2014).

'Chatham House Report' investigated the range of cyber security challenges at nuclear facilities (Baylon et al., 2015). According to this report, one of the major problems in the nuclear industry is that the industry is situated in a very early stage to deal with cyber security issues. The main reason why this problem happens is because cyber security has received less attention than other safety problems have. In addition, the late adoption of DI&C systems has resulted in the lower level of cyber security advancements in the nuclear industry than those in other industries. Also, limited

* Corresponding author at: Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291, Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea.
E-mail addresses: lcy5228@kaist.ac.kr (C. Lee), yimhobin@kepco-enc.com (H.B. Yim), phseong@kaist.ac.kr (P.H. Seong).

https://doi.org/10.1016/j.anucene.2017.11.002
0306-4549/

incident disclosure and unclear collaboration among related corporations have made it difficult to assess the true extent of problems of cyber security issues.

Many regulatory documents, guides and standards were already published in order to provide useful information about cyber security issues in the nuclear industry, such as RG 5.71 by the U.S. Nuclear Regulatory Commission (U.S. NRC, 2010) and RS-015 by Korea Institute of Nuclear nonproliferation and Control (KINAC, 2014). These documents include cyber security plans and methods for the cyber security assessment, and comprehensive sets of security controls. Technical security control requirements analysis can be also provided based on these documents (Song et al., 2013).

However, difficulties still exist when deciding which security controls are needed and defining appropriate security control requirements (Song et al., 2013). The main reasons are; practical examples for the application of security controls are not available to system designers, and methods that can help assess how much security is improved if a specific control is applied are not included.

Although several quantitative methods were developed to evaluate security controls in other industries, these methods cannot be directly applied to NPPs, because quantifying or rating cyber risk is hard to be validated in NPP DI&C systems whereas relatively easy in the IT industry (Song et al., 2013). Also, availability of safety functions which must be maintained when facing unexpected intrusions should be considered as the most important factor in the nuclear industry rather than financial loss or information confidentiality. There has also been attempts to evaluate security controls using relationship between vulnerabilities and security controls in the nuclear industry (Shin et al., 2015). Difficulty in clearly relating the direct correlation between vulnerabilities and security controls, nonetheless, always remains in such complex NPPs. There is also a biased need to focus more on availability of plant safety functions than on causes. Moreover, the evaluation of security controls has been heavily relied on human experts' experience and judgement in the nuclear industry that objective evaluation results are hardly expected.

To overcome this shortcoming, the systematic as well as quantitative method for evaluating the efficacy of security controls for NPPs is proposed; ***In***trusion ***To***lerance based ***C***yber ***S***ecurity ***I***ndex (*InTo-CSI*). The definition of *InTo-CSI*, which represents the efficacy of security controls, is described in the second section. The intrusion tolerant concept was applied to the evaluation method considering availability of safety functions as the prime concern. *InTo-CSI* uses failure probability of intrusion tolerant strategies based on the intrusion tolerant concept. The concept of Mean Time To Compromise (MTTC) was also adopted for quantifying abstract contents. In Section 3, the validity of the suggested method was proven by conducting a case study on the Digital Plant Protection System (DPPS) with three kinds of security controls specified on RG 5.71. Conclusions are presented in the last part of the study.

2. Intrusion Tolerance based Cyber Security Index (*InTo-CSI*)

2.1. Definition

Intrusion Tolerance based Cyber Security Index (*InTo-CSI*) is an index, as the name specifies, for indicating the efficacy of security controls. The index was defined through relative comparison of two security states of the same system: A system without any cyber security controls, namely the baseline system, and a system with scrutiny controls, called the enhanced system. The estimation of how much the system is improved in terms of cyber security was fulfilled by comparing the security states of baseline system to the enhanced system. Most quantitative risk assessment models define risk as the product of probability and consequence, and use the reduced ratio of risk as a quantitative indicator (Ralston et al., 2007). In this study, the reduced ratio of risk was replaced by the reduced ratio of probability, because the cyber risk tends to decrease when the likelihood of successful attacks decreases. Another reason is that, since security controls are a kind of preventive measures, consequence caused by a damaged system cannot be evidently mitigated by applying security controls (Nzoukou et al., 2013). Therefore, *InTo-CSI* was defined as the reduction ratio of probability that a cyber-attack damages a target system.

$$InTo - CSI = 1 - \frac{P_{Enhanced}}{P_{Baseline}} \quad (1)$$

Where,

- $P_{Baseline}$: Failure probability of securing the current system from cyber-attacks
- $P_{Enhanced}$: Failure probability of securing the enhanced system from cyber-attacks
- $P_{Enhanced}$ may have a smaller value than $P_{Baseline}$ if applied security controls have a positive effect on securing a target system.

Previous approaches to cyber security have mainly focused on enhancing and fortifying the protection of target systems (Madan et al., 2004). Hence, as far as vulnerability is concerned, damages may follow one after another and eventually cause critical accidents. Regulatory documents specified to prevent this situation that the defense-in-depth protective strategy should be maintained to ensure the capability of not only protection and detection, but also response and recover from cyber-attacks (NRC, 2010; KINAC, 2014). With this regards, the intrusion tolerant concept is considered in the evaluation method. An intrusion tolerant system is a system which provides the minimum level of safe operation when facing unexpected intrusions. It allows finite probability where the system's security fails so that the security failure can be more easily detected, and adverse effects of the attack is nullified (Madan et al., 2004). In addition, the system should be designed in accordance with its priorities. For example, the system must be designed to stop functions when an attack is detected if the aim is to protect confidentiality or data integrity. On the other hand, if the goal is to protect availability of system's essential functions, the system design must be focused on maintaining essential functions. Availability of system's essential functions is the first priority in safety critical systems, such as DI&C in the nuclear industry. Therefore, five intrusion tolerant strategies which aim to protect availability of system's essential functions were investigated based on behaviors of intrusion tolerant systems (Madan et al., 2004).

- Resistance strategy: to make exploitation of vulnerabilities difficult
- Detection strategy: to detect a valid attack in the exploitation phase
- Back-up strategy: to have enough back-up systems to enable the delivery of the error free service
- Elimination strategy: to have measures for eliminating risk sources while maintaining system's functions
- GD (Graceful-Degradation) strategy: to maintain only system's essential functions allowing degradation of less important functions.

An event tree was constructed based on these intrusion tolerant strategies as Fig. 1. The initiating event is a known-type of cyber-attack that could affect essential functions of a target system. If an attempted known cyber-attack successes in exploitation of vulnerability, the security failure will be taken into account, and the attempted attack is going to be considered as a valid attack.